2767
2132
#12
KW

In the United States Patent and Trademark Office

Serial Number:	09/081,872
Appn. Filed:	05/20/98
Applicant(s):	John H. Messing
Appn. Title:	Electronic Signature Program
Examiner:	Douglas J. Meislahn
Group Art Unit:	2767

Mailed: August 14, 2002

At: Tucson, Arizona

Summary of Telephonic Interview

Assistant Commissioner for Patents
Washington, District of Columbia 20231

Sir:

This is applicant's summary of the telephonic Interview of June 10, 2002, provided as per the attachment PTO 413 of the OA mailed June 20, 2002.

The Applicant had given the Examiner access to a demonstration website in order to demonstrate the invention without the presence of the Applicant. The demonstration was successfully accessed and run by the Examiner. The telephonic interview followed.

The applicant asked if the Examiner had received a written document consisting of a Correction to Amendment C, particularly the last part of it which referenced an error in the Amendment as follows: "Page 28, l. 23, the following ultimate sentence was inadvertently omitted during word processing and should be inserted:

'The fact that Kocher teaches the use of symmetric ciphers to encrypt documents for confidentiality purposes during storage in the archive (Col. 10, lines 32-36) but does not also suggest the use DIVs or TTIs as encryption keys simultaneously to sign symmetrically during encryption as a MAC signature, establishes the novelty of former Claim 48 now Claim 63 over Kocher.'"

The Examiner searched for the document, and reported that he believed he had located it in the file.

In response to a written argument of the Applicant in an earlier OA response, the Examiner stated words to the effect that under Section 102, a rejection did not have to be based upon all of the elements of the prior art matching the invention of the application, and vice-versa in order to support a rejection. The Applicant took this to mean that the Examiner did not agree with the citation of legal authorities of the Applicant in the response to the most recent Office Action.

The Applicant reported to the Examiner that the demonstration illustrated how the symmetric encryption worked together with the preferred asymmetric embodiment of the invention. Applicant attempted to clarify how the symmetric encryption works together with the preferred asymmetric embodiment of the invention, and not simply as an alternative to it. The asymmetrically encrypted RSA signature value returned by the web program is in turn itself encrypted by a second symmetric cipher. The symmetric cipher is indirectly derived from the identity of the signer in the formulation of the GUID. In order to be able to decrypt the asymmetric signature value and verify the signature, the symmetric encryption involving the signer's identity must be decrypted first; otherwise, asymmetric signature verification using a public key is impossible. In this way, the identity of the signer becomes cryptographically wrapped around the asymmetric signature of the server's key; hence the terminology in the specification of a "digital wrapper." The Applicant attempted to point out that this combination in the telephone conversation with the Examiner in order to point out that it had the further advantage of protecting the private key of the server from a potential vulnerability otherwise occasioned from its constant use for signature transactions. Without the symmetric digital wrapper that changed with each signer transaction, an attacker might be able to deduce the private key attributes from an examination of a myriad of signatures and hash values. The symmetrically encrypted signature value also can serve to protect the underlying asymmetric signature at a future time when a factoring attack on asymmetric RSA signatures by significantly more powerful computers may become computationally feasible. The symmetric encryption of the returned asymmetric signature value may act as an added shield to protect the asymmetric private key from a factoring attack as the symmetric enciphering wrapper cloaks the asymmetric signature value, hiding it from the

attacker. The Applicant opined to the Examiner this embodiment of the invention was novel as against prior art.

The interview cordially ended by mutual agreement, as there was nothing further to discuss.

Very respectfully,

John H. Messing
Postal Address:
3900 E. Broadway Blvd., Suite 201
Tucson, AZ 85712
U.S. Citizen
Tel.: (520) 547-7933
Or (520) 529-3275
Fax: (520) 529-3204
Email: jmessing@law-on-line.com